

DA PRIVACY IMPACT ASSESSMENT (PIA)

1. DA organizational name (APMS Sub Organization name):

U.S. Army Corps of Engineers (USACE)

2. Name of Information Technology (IT) System (APMS System name):

Operations & Maintenance Business Information Link Plus (OMBILPlus)

3. Budget System Identification Number (SNAP-IT Initiative Number):

9997

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR) :

3702

5. IT Investment (OMB Circular A11) Unique Identifier (if applicable):

202-00-01-02-01-1031-00

6. Privacy Act System of Records Notice Identifier (if applicable):

A0015-2-2CE
A1130-2-442CE
A1145aCE
A1145bCE

7. OMB Information Collection Requirement Number (if applicable) and expiration date:

OMB 0710-0003 Army Permit, expiration date 30 April 2008

8. Type of Authority to collect information (statutory or otherwise):

Section 234 of the Flood Control Act of 1970 (Pub. L. 91-611; 84 Stat. 1818).
5 U.S.C. 5901-5903;
16 U.S.C. 460d;
31 U.S.C. 483a;
33 U.S.C. 652;
33 U.S.C. 1251 et seq;
42 U.S.C. 4321, 4331-4335, 4341-4347;
E.O. 9397 (SSN)

E.O. 11752

Harbor Act of March 3, 1899 (sections 9, 10, and 14);

Federal Water Pollution Control Act Amendments of 1972 (section 404);

Marine Protection, Research and Sanctuaries Act of 1972 (section 103);

1899 (33 U.S.C. 401, et seq.);

Section 10 (33 U.S.C. 403).

Army Regulation 385-40 Accident and Reporting

USACE Engineer Regulation (ER) 190-1-50 Law Enforcement Policy

USACE ER 670-2-2

USACE ER 670-2-3

USACE ER1130-2-442

9. Provide a brief summary or overview of the IT system:

OMBIL Plus is a corporate, automated information system (AIS) that standardizes, integrates and modernizes legacy AISs to provide business information and performance for the USACE Civil Works Operations projects. This includes the restructuring of data to align with the business areas of navigation, hydropower, recreation, flood damage reduction, environment, regulatory and water supply. The AIS uses a data warehouse to merge financial, activity, inventory and output data to create performance measures of efficiency and effectiveness.

10. Describe what information in identifiable form will be collected and the nature and source of the information:

Name, street, city, state, zip code, phone number, fax number, e-mail address, height, weight, eye color, date of birth, drivers license number, SSN, age, gender, and accident information. The source of the information is from the individual.

11. Describe how the information will be collected:

Web-based program. Information is obtained from the individual via an interview or form and then manually entered on behalf of the users by USACE employees.

12. Describe the requirement, why the information in identifiable form is to be collected and how the information will be used:

The Army needs the information in order to process permit applications, issue citations and to create and process accident reports and criminal offense reports. The mission of the regulatory system is to assist in the processing of Army permit applications from citizens, businesses, state, local and tribal governments in order to allow reasonable development while protecting the Nation's waters and wetlands. Park rangers (Army employees) use the system to collect data about individuals to issue citations to the public for misuse of USACE recreation areas or for offenses committed. The Safety Office collects data about accidents on USACE property, conducts accident investigations, and provides reports for trend analysis by accident type.

14. Describe whether the system derives or creates new data about individuals through aggregation:

This system does not create new data about individuals through aggregation

15. Describe with whom the information in identifiable form will be shared, both within DA and outside DA:

Information will be available to authorized users with a need to know in order to perform official government duties. Internal Department of Defense (DoD) agencies that would obtain access to personal information in this system, on request, in support of an authorized investigation or audit, may include DoD/Army Inspector Generals, Defense Criminal Investigation Service, Army Staff Principals in the chain of command, and Army Audit Agency,. In addition, the DoD blanket routine uses apply to this system. External entities that may obtain access to personal information include local, state, tribal, and civilian Federal regulatory agencies, e.g. Environmental Protection Agency (EPA), law enforcement and court systems.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form:

Furnishing this information is voluntary based on the individual's desire to obtain a permit. If individuals become the subject of a safety or legal investigation, then the individual is required by law to self-identify; other information may be obtained from the individual or from other sources.

17. Describe the process regarding how the individual is to grant consent:

A privacy act advisory is provided to individuals.

18. Describe any information that is provided to an individual and the format of such information and means of delivery:

Individuals are provided approved/disapproved permits and citations in hardcopy format.

19. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form:

Computerized records are maintained in a controlled area accessible only to authorized personnel. Entry is restricted by the use of locks, guards, and administrative procedures. Access to personal information is limited to those who require the records in the performance of their official duties, and to the individuals who are the subjects of

the record or their authorized representatives. Access to personal information is further restricted by the use of unique logon and passwords, which are changed periodically. This system has a current certification and accreditation. The system resides on secure Army and Federal government facilities within secured facilities.

20. Identify whether the IT system or collection of information will require a System of Records notice. If not published, state when publication of the notice will occur:

Existing Army SORNs apply (see #6 above).

21. Describe/evaluate any potential privacy risks the collection, use, and sharing of the information in identifiable form:

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in the collection, use and sharing of information.

22. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals:

There are no risks in providing individual the opportunity to object or consent.

23. Describe/evaluate any risks posed by the adopted security measures:

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal.

24. State classification of information/system and whether the PIA should be published or not. If not, provide rationale:

Unclassified/FOUO. The PIA may be published.

25. If a PIA is planned for publication, state whether it will be published in full or summary form:

The PIA may be published in its entirety.